UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/608,986	06/30/2000	Jin Su	10559/214001/P8707	1439

21552 7590 04/15/2004

MADSON & METCALF
GATEWAY TOWER WEST
SUITE 900
15 WEST SOUTH TEMPLE
SALT LAKE CITY, UT 84101

EXAMINER	
SIMITOSKI, MICHAEL J	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 04/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

8/24

Office Action Summary	Application No. 09/608,986	Applicant(s) SU ET AL.	
	Examiner Michael J Simitoski	Art Unit 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-27* is/are pending in the application.

4a) Of the above claim(s) *1-7* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *8-27* is/are rejected.

7)☒ Claim(s) *17* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 June 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-27 are pending.

Election/Restrictions

2. Applicant's election without traverse of group II (claims 8-27) in Paper No. 10 is acknowledged.

3. Claims 1-7 withdrawn from further consideration pursuant to 37 CFR 1.142(b), as being drawn to a nonelected invention, there being no allowable generic or linking claim. Applicant timely traversed the restriction (election) requirement in Paper No. 10.

Drawings

4. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the "matching a signature on the submitted certificate with a signature on the trusted certificate" (claim 12) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

Claim Objections

5. Claim 17 is objected to because of the following informalities:

a. "registering new authentication session" should be replaced with "registering a new authentication session".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claim 12 is rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The recited limitation "matching a signature on the submitted certificate with a signature on the trusted certificate" is not found in the specification. *For the purposes of this Office Action, "matching a signature on the submitted certificate with a signature on the trusted certificate" will be considered as equivalent with "checking the certificate's signature with the trusted core's certificate" as described in the specification (page 8, ¶2), checking being defined by the following taken from The American Heritage College Dictionary*:

1. The act or an instance of inspecting or testing, as for accuracy or quality; examination.
2. A standard for inspecting or evaluating; a test.

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 13-15 & 23 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Claims 13 & 14 recite the limitation "using the encrypted key to encrypt communication", however Fig. 4 depicts sending an encrypted symmetric key (symmetric key encrypted with the client's public key) to the client and using the symmetric key (rather than the claimed "encrypted key") to encrypt communication; the claim suggests that an encrypted key is used (as a key) to encrypt communication, wherein the specifications suggest that a decrypted key (that was previous encrypted) is used to encrypt communication. *For the purposes of this Office Action, "using the encrypted key to encrypt communication" is understood to mean "using the key to encrypt communication".* Claim 15 is rejected based on its dependence upon claim 14.

b. Claim 23 recites the limitation "the authentication" in line 3. There is insufficient antecedent basis for this limitation in the claim. *For the purposes of this Office Action, "the authentication" is understood to mean "the authentication token".*

Claim Rejections - 35 USC § 102

10. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claim 14 is rejected under 35 U.S.C. 102(b) as being anticipated by Applied Cryptography, Second Edition by Schneier.

Regarding claim 14, as best understood, Schneier (page 48, § Key Exchange with Public-Key Cryptography) discloses generating a key/random session key (step 2), encrypting the key with a client's/Bob's public key (step 2), sending an encrypted key to a client/Bob (step 2) and using the encrypted key to encrypt communication (step 4).

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 8-12, 16-22 & 24-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 5,657,390 to Elgamal et al. (Elgamal) in view of "Single Sign-On Using Cookies for Web Applications" by Samar.

Regarding claims 8 & 24, Elgamal discloses submitting a request to access a node (Fig. 12A), directing to submit a certificate (Fig. 4, client-hello), verifying the submitted certificate (col. 7, lines 20-40), performing a challenge (Fig. 4, client-hello) and generating a response to the challenge (Fig. 4, server-verify). Elgamal does not disclose saving the response as a named cookie. However, Samar teaches that storing response data (cookie id and cookie integrity check) (Fig. 1 & §6.1.2) is advantageous for single sign-on because no extra software has to be installed and it is independent from the authentication mechanism (§4). Therefore, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication scheme used by Elgamal with the SSO architecture to store the response as a named cookie. One of ordinary skill in the art would have been motivated to perform such a modification to enable single sign-on without the need for extra software or specific authentication mechanisms, as taught by Samar (Fig. 1 & §4). Elgamal, as modified, does not explicitly disclose verifying the submitted certificate with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 9 & 25, Elgamal, as modified above, discloses using the cookie/response as a security token (Samar, §6.1).

Regarding claim 10, Elgamal, as modified above, discloses the security token being used to propagate initial authentication (Samar, §6.1).

Regarding claim 11, Elgamal, as modified above, discloses creating a connection session if the certificate is valid (Fig. 4 & col. 8, lines 54-61).

Regarding claim 12, Elgamal, as modified above, Elgamal lacks checking the certificate's signature with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 16 & 26, Elgamal discloses submitting a request to access a node (Fig. 12A), directing to submit a certificate (Fig. 4, client-hello), verifying the submitted certificate (col. 7, lines 20-40), performing a challenge (Fig. 4, client-hello) and generating a response to the challenge (Fig. 4, server-verify). Elgamal further discloses using the SSL library (col. 34, lines 39-49). Elgamal does not disclose saving the response as a named cookie. However, Samar teaches that storing response data (cookie id and cookie integrity check) (Fig. 1 & §6.1.2) is advantageous for single sign-on because no extra software has to be installed and it is independent from the authentication mechanism (§4). The cookie is used as an authentication token (§6.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the authentication scheme used by Elgamal with the SSO architecture to store the response as a named cookie. One of ordinary skill in the art would

have been motivated to perform such a modification to enable single sign-on without the need for extra software or specific authentication mechanisms, as taught by Samar (Fig. 1 & §4). Elgamal, as modified, does not explicitly disclose verifying the submitted certificate with a trusted certificate, but discloses that the certificate is used to verify the authenticity of the server using well known techniques (col. 7, lines 20-40). The examiner takes Official Notice that retrieving a trusted certificate (self-signed certificate to obtain the authentic public key of a certificate authority) and verifying a submitted certificate based on the retrieved public key is old and well established in the art of cryptography as a method of securely authenticating an entity using a trusted third party. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to verify the submitted certificate with a trusted certificate. One of ordinary skill in the art would have been motivated to perform such a modification to verify the authenticity of the submitted certificate via a trusted third party. This advantage is well known to those skilled in the art.

Regarding claims 17, 18 & 27, Elgamal lacks creating a new authentication session with the authentication token. However, Samar discloses a centralized login server approach to single sign-on where an initial web server redirects a client to a new web server that has access to a cookie server (Fig. 2). The new web server then redirects the client back to the first server with the cookie where the web server verifies the cookie and returns a session cookie (creating and registering a new authentication session). The initial web server validates the new authentication session using the authentication token/cookie (Fig. 2 & §8). The benefit of the centralized login server is that all authentication information for the user is consolidated (§8). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to

create and register a new authentication session. One of ordinary skill in the art would have been motivated to perform such a modification to enable the consolidation of all authentication information, as taught by Samar (Fig. 2 & §8).

Regarding claim 19, Elgamal lacks indicating a failure status to a client if verification fails. However, the examiner takes Official Notice that indicating a failure status (such as error messages) to a client if a verification/authentication, etc. fails is old and well established in the art of cryptography and network security as a means to notify a client that the verification has failed. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to indicate a failure status to a client if verification fails. One of ordinary skill in the art would have been motivated to perform such a modification to indicate to the client that verification has failed. This advantage is well known to those skilled in the art.

Regarding claim 20, Elgamal, as modified above, discloses the challenge being a random number (col. 7, lines 13-19).

Regarding claim 21, Elgamal, as modified above, discloses receiving an address/URL of a node and checking to determine if the address is protected (SSL to be used for information retrieval) (Fig. 12A).

Regarding claim 22, Elgamal lacks determining if the authentication token is already present. However, Samar teaches that SSO is useful so that users to not have to enter usernames and passwords many times per day (§1). Samar further teaches that in a centralized login server approach, a server first must check to see if a cookie was presented (authentication token already present) (§8 & Fig. 2) (otherwise the system would not be SSO). The centralized approach brings the benefit of authentication and management centrality (§8). Therefore, it would have

been obvious to one having ordinary skill in the art at the time the invention was made to determine if the authentication token is already present. One of ordinary skill in the art would have been motivated to perform such a modification to implement an SSO system to prevent repeated username and password combination uses, as taught by Samar (§1, §8 & Fig. 2).

14. Claim 13, as best understood, is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Samar, as applied to claim 8 above, in further view of Applied Cryptography, Second Edition by Schneier. Elgamal lacks generating a key, encrypting the key with a client's public key, sending an encrypted key to a client and using the encrypted key to encrypt communications. However, Schneier (page 48, § Key Exchange with Public-Key Cryptography) teaches generating a key/random session key (step 2), encrypting the key with a client's/Bob's public key (step 2), sending an encrypted key to a client/Bob (step 2) and using the encrypted key to encrypt communication (step 4). Schneier teaches that this is a basic key-exchange scheme used with Public Key cryptography to exchange a session key used to communicate securely (page 48, § Key Exchange with Public-Key Cryptography). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to generate a key, encrypt the key with a client's public key, send an encrypted key to a client and use the encrypted key to encrypt communications. One of ordinary skill in the art would have been motivated to perform such a modification to exchange a session key to encrypt communications, as taught by Schneier (page 48, § Key Exchange with Public-Key Cryptography).

15. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier, as applied to claim 14 above, in further view of U.S. Patent 6,199,113 to Alegre et al. (Alegre) in further view of "HTTP State Management Mechanism" by Kristol et al. (Kristol). Schneier teaches only a method of key exchange and therefore does not teach implementation details. Hence, Schneier lacks sending the key using a hypertext transfer protocol (HTTP) header. However, Alegre teaches that authentication data (cookie) can be stored at a browser to automatically authenticate a user during a session (col. 4, lines 1-7). Alegre teaches that a session key is stored in a cookie at the browser (col. 4, lines 31-54). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use Schneier's key exchange protocol to exchange a session key and store it in the browser. One of ordinary skill in the art would have been motivated to perform such a modification to gain the benefit of automatically authenticating a user during a session, as taught by Alegre (col. 4, lines 1-54). Schneier, as modified, lacks specific disclosure of sending the key in an HTTP header. However, Kristol teaches that a cookie is transmitted via HTTP headers (§4.2) in HTTP state management. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to specifically send the key using HTTP headers. One of ordinary skill in the art would have been motivated to perform such a modification to set the cookie according to the HTTP/1.0 and HTTP State Management Mechanisms standards, as taught by Kristol.

16. Claim 23 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal in view of Samar, as applied to claim 22 above, in further view of Handbook of Applied Cryptography

by Menezes et al. (Menezes). Elgamal discloses a system, as modified above, but lacks determining if a client is on an access control list if the authentication is present and valid. However, Menezes teaches that certificates should be revoked if evidence exists that suggests that the certificate should no longer be issued (§13.7.2). Menezes further teaches that certificate authorities publish certificate revocation lists to be checked for invalid certificates (§13.6.3) because distributed copies exist and may not immediately be aware of the need for revocation (§13.6.3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to determine if the client/certificate is on an access control list/certificate revocation list after the authentication token is deemed valid (signature contained in the certificate is successfully decrypted using the public key of the authority and compared to the data over which the signature has been taken). One of ordinary skill in the art would have been motivated to perform such a modification to make sure the distributed client certificate has been not revoked, as taught by Menezes (§13.6.3 & §13.7.2).

Conclusion

17. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. The '768, '322 & '040 references are cited for teaching using cookies/authentication tokens to store session keys/authentication-related data/credentials.

b. The Fielding reference was cited for teaching using cookies in web applications.

c. The Ford reference was cited for teaching PKI-based certificate applications.

18. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
April 6, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER